USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 10/28/14

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- against -

FRANK DiTOMASSO,

Defendant.

OPINION AND ORDER

14-cr-160 (SAS)

SHIRA A. SCHEINDLIN, U.S.D.J.:

I. INTRODUCTION

Frank DiTomasso faces criminal charges for the production and transportation of child pornography. Much of the government's case against DiTomasso depends on evidence found on his computer — evidence that he claims was obtained in violation of the Fourth Amendment. Accordingly, DiTomasso has moved to suppress (1) evidence obtained when internet service provider ("ISP")[1] American Online ("AOL") examined the content of his email, (2) evidence

---

[1] The exact meaning of "Internet Service Provider" is unclear. Wikipedia defines the term broadly — to encompass not only entities that provide "internet service," thereby allowing consumers to get online (such as Comcast and Time Warner), but also entities that provide internet-*based* services (such as Google and AOL). *See* "Internet Service Provider," *Wikipedia*, available at http://en.wikipedia.org/wiki/Internet_service_provider (last updated Sept. 24, 2014). The parties here have followed suit, adopting the broader interpretation. This Opinion does the same.

obtained when ISP Omegle.com LLC ("Omegle") examined the content of his chats, and (3) all "information and tangible and intangible evidence obtained through subsequent searches by [law enforcement]" as fruit of the poisonous tree.[2]

This Opinion addresses two questions. *First*, it addresses the threshold question of whether DiTomasso had an expectation of privacy in the content of his emails and chats. If so, his Fourth Amendment challenge to AOL's and Omegle's conduct may proceed. If not, the challenge fails as a matter of law. *Second*, it addresses whether DiTomasso, by agreeing to AOL's and Omegle's respective terms of use, consented to a search of his emails and/or his chats.

For the reasons set forth below, DiTomasso's motion to suppress is DENIED in part.

II. BACKGROUND

A. AOL Emails

DiTomasso has an AOL email account — frankieinnyc1@aol.com. When AOL users send or receive emails that contain attachments, AOL runs two background monitoring systems designed to scan for illicit material, including, but not limited to, child pornography.[3] The programs work by assigning "hash

---

[2] Memorandum of Law in Support of Motion to Suppress, at 1.

[3] *See* Declaration of Greg Phillips, Senior Technical Security Investigator for the Public Safety and Criminal Investigation at AOL ("Phillips

numbers" to image and video files. In essence, hash numbers are unique number-strings that can be used to archive packets of data — "fingerprint[s]" for electronic media.[4]

AOL employs two different hashing programs. The first — the Image Detection and Filtering Process ("IDFP") — sweeps for one-to-one matches with known child pornography.[5] If an attached file is a one-to-one match, the email is quarantined — *i.e.*, diverted from the recipient's inbox — and an automatic report is generated and sent to the National Center for Missing and Exploited Children ("NCMEC report").[6]

AOL's second hashing program — "photoDNA" — looks for similarities among hash numbers.[7] If photoDNA identifies an attachment with a hash number close enough to known child pornography to raise alarm, the email is once again quarantined, and "an AOL employee reviews the flagged file to confirm

---

Decl."), Exhibit ("Ex.") F to Government's Memorandum in Opposition to the Motion to Suppress ("Opp. Mem."), ¶¶ 4-6.

[4] *Id.* ¶ 5.

[5] *See id.* ¶¶ 7-8.

[6] *See id.* ¶ 7.

[7] *See id.* ¶ 9.

the presence of apparent child pornography."[8] Once the presence of apparent child pornography is confirmed, the employee "submit[s] a [NCMEC report],"[9] and the file's hash number is entered into the IDFP database.

On August 17, 2012, two emails intended for frankieinnyc1@aol.com were hashed and quarantined, giving rise to two corresponding NCMEC reports. The first email, which formed the basis of NCMEC report #1560137, was hashed using photoDNA — and its contents were reviewed by an AOL employee.[10] The second email, which formed the basis of NCMEC report #1558963, was hashed using IDFP.[11] No AOL employee reviewed its contents.

B. AOL's Privacy Policy

At the time of the disputed searches, AOL's privacy policy and terms of use required users to assent to the following conditions. *First*, they forbade users from "post[ing] content that contains explicit or graphic descriptions or accounts of sexual acts or is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or tortious."[12] *Second*, AOL's

---

8 *Id.* ¶ 11.

9 *Id.*

10 *See* Opp. Mem. at 3.

11 *See id.*

12 AOL Terms of Service, Ex. I to Opp. Mem., at 1.

terms provided that "AOL reserves the right to take any action it deems warranted" in response to illegal behavior, including "terminat[ing] accounts and cooperat[ing] with law enforcement."[13] *Third*, AOL's terms made clear that if users "disclose information about [themselves] publicly . . . others outside of AOL may obtain access to [such] information," and furthermore, that AOL itself may disclose to others — including law enforcement — "information [that is] relevant to a crime that has been or is being committed."[14]

C. Omegle Chats

Omegle.com is an online platform that "randomly pairs a user in a one-on-one session with a stranger, and allows strangers to communicate via text and video chats."[15] Omegle monitors "for inappropriate content . . . by capturing snapshots from chats that are conducted on Omegle,"[16] which are then "analyze[d]" by an automated program "for content that is likely to be inappropriate, including, but not limited to, child pornography."[17] When the automated program flags

---

[13] AOL Member Community Guidelines ("AOL Guidelines"), Ex. G to Opp. Mem., at 1-2.

[14] AOL Privacy Policy, Ex. H to Opp. Mem., at 2.

[15] Declaration of Lief Brooks, Founder of Omegle.com, Ex. C to Opp. Mem., ¶ 2.

[16] *Id.* ¶ 3.

[17] *Id.* ¶ 4.

inappropriate content, the chats are "passed on to two human reviewers,"[18] and if a reviewer finds evidence of child pornography, a NCMEC report is filed.[19]

On three separate occasions — November 30, 2012, January 4, 2013, and December 11, 2013 — snapshots of DiTomasso's Omegle chats were flagged for evidence of child pornography. This led to the filing of three NCMEC reports: #1704143, #1741964, and #2235394, respectively.[20]

D. Omegle's Privacy Policy

At the time of the disputed searches, Omegle's privacy policy set forth the following conditions. *First*, Omegle's policy explained that Omegle keeps "record[s] of the IP addresses involved in every chat."[21] The policy articulated numerous reasons for maintaining such records — including "for the purpose of law enforcement."[22] *Second*, Omegle's policy also made clear that it engages in two forms of monitoring distinct from its IP record-keeping, which are intended for

---

[18] *Id.*

[19] *See id.* ¶ 5.

[20] *See* Opp. Mem. at 3.

[21] Omegle.com Privacy Policy ("Omegle Policy"), Ex. E to Opp. Mem. at 1.

[22] *Id.* In fact, users' IP addresses are recorded with the explicit "inten[tion] [of] be[ing] used for the purpose of law enforcement." *Id.*

"quality control purposes."[23] The first is that messages flagged as spam "may be read by a human being to improve Omegle's anti-spam software."[24] The second is that "[w]ebcam videos may be captured from Omegle video charts . . . and monitored," on an ad hoc basis, "for misbehavior."[25] *Third*, Omegle's policy cautioned users to be "careful about what information [they] reveal" during chats, because "strangers can potentially tell other people anything you tell them."[26]

E. DiTomasso's Probation

At the time of the disputed searches, DiTomasso was on probation in connection with a 2010 conviction for possession of child pornography.[27] The probation terms — to which DiTomasso consented — required, among other things, that he "[p]ermit [his] probation officer or their designee to inspect and access your computer at anytime, [] includ[ing] storage devices and any other media."[28]

---

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* Order and Conditions of Probation for Frank DiTomasso ("Probation Order"), Ex. J to Opp. Mem.

[28] *Id.* at 2 ¶ U.

III. APPLICABLE LAW

A. Expectations of Privacy in General

The Fourth Amendment to the United States Constitution protects "the right of the people to be secure . . . against unreasonable searches and seizures."[29] Whether an investigative activity qualifies as a "search" — and triggers Fourth Amendment scrutiny — depends on subjective expectations of privacy.[30] If (1) an individual expects that information will remain private, and (2) society is "prepared to recognize [that expectation] as 'reasonable,'"[31] the Fourth Amendment regulates the investigation of that information by law enforcement.

Constitutionally-recognized "expectations of privacy" differ in two important respects from the "mere expectation . . . that certain facts will not come to the attention of the authorities."[32] *First*, the Fourth Amendment does not protect ill-advised trust. It provides no recourse for "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[33] By

---

[29] U.S. CONST. amend. IV.

[30] *See United States v. Katz*, 389 U.S. 347, 360-62 (1967) (Harlan J., concurring).

[31] *Id.* at 361.

[32] *United States v. Jacobsen*, 466 U.S. 109, 122 (1984).

[33] *Hoffa v. United States*, 385 U.S. 293, 302 (1966).

disclosing sensitive information to someone else, one runs the risk that the other person will reveal the information to law enforcement.

Second, "a person has no legitimate expectation of privacy in information that he voluntarily turns over to third parties."[34] Because this principle, if taken to its logical endpoint, would erode nearly all privacy protections, in *Smith v. Maryland* the Supreme Court distinguished between (1) the "*contents* of communication[]" and (2) the ancillary information that the act of communication incidentally discloses.[35] Today, this distinction is often described as the difference between data and metadata. While the former retains Fourth Amendment protection even if disclosed to a third party, the latter loses its protection immediately once disclosed.

B. Diminished Expectations of Privacy While on Probation

"Probationers and parolees are subject to 'a degree of impingement upon privacy that would not be constitutional if applied to the public at large.'"[36] In *United States v. Knights*, the Supreme Court held that probation agreements containing consent-to-search provisions "significantly diminish[] [the

---

[34] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

[35] *Id.* at 741 (emphasis added).

[36] *Unites States v. Newton*, 369 F.3d 659, 665 (2d Cir. 2004) (citing *Griffin v. Wisconsin*, 483 U.S. 868, 875 (1987)).

probationer's] expectation of privacy."[37] In so holding, the Court explicitly reserved the question of whether a consent-to-search provision simply "diminishe[s], or completely eliminate[s], [the probationer's] expectation of privacy"[38] — and correspondingly, whether "a search by a law enforcement officer without any individualized suspicion would [satisfy] the reasonableness requirement of the Fourth Amendment."[39]

Elaborating on these principles, the Second Circuit has explained that "persons on supervised release who sign [] documents [consenting to future searches of their home] manifest an awareness that supervision can include intrusions into their residence and, thus, have 'a severely diminished expectation of privacy.'"[40] Furthermore, the Second Circuit has also held that home visits by probation officers — as opposed to full probationary searches — do not even require "reasonable suspicion," because home visits are so much "less intrusive."[41]

C. Fourth Amendment Standing

---

[37] 534 U.S. 112, 120 (2001).

[38] *Id.* at 120 n.6.

[39] *Id.*

[40] *Newton*, 369 F.3d at 665 (citing *United States v. Reyes*, 283 F.3d 446, 461 (2d Cir. 2002)).

[41] *United States v. Lifshitz*, 369 F.3d 173, 182 (2d Cir. 2004) (internal citations omitted).

"Fourth Amendment rights are personal rights which . . . may not be vicariously asserted."[42] A person lacks standing to raise Fourth Amendment claims if the disputed evidence was procured "by a search of a third person's premises or property" rather than his own premises or property.[43]

D. Consent to Search

"[T]he ultimate touchstone of the Fourth Amendment is reasonableness."[44] Even if a search would otherwise be invalid — because it encroaches unreasonably on one's expectations of privacy — "an individual may *consent* to a search, thereby rendering it reasonable."[45] Consent only renders a search reasonable, however, if "the consent was 'a product of [the] individual's free and unconstrained choice.'"[46] This test is not as exacting as the "knowing and

---

[42] *Alderman v. United States*, 394 U.S. 165, 174 (1969).

[43] *Rakas v. Illinois*, 439 U.S. 128, 134 (1978).

[44] *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (internal citations omitted).

[45] *United States v. Garcia*, 56 F.3d 418, 422 (2d Cir. 1995) (emphasis added). *Accord Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973) ("[A] search conducted pursuant to a valid consent is constitutionally permissible.").

[46] *Garcia*, 56 F.3d at 422 (quoting *United States v. Wilson*, 11 F.3d 346, 352 (2d Cir. 1993)).

intelligent waiver" standard familiar to other areas of criminal procedure.[47] Rather, "so long as [consent is] not coerce[d], a search conducted on the basis of consent is not [] unreasonable."[48] Ultimately, whether consent was properly given is an "objective" question: it depends on how "the typical reasonable person [would understand]" the conduct supposedly amounting to consent.[49]

III. DISCUSSION

A. DiTomasso's Expectations of Privacy

In assessing DiTomasso's expectations of privacy, three questions arise. *First*, did DiTomasso have an expectation of privacy in his electronic communications? *Second*, did DiTomasso's probation agreement, granting his probation officer (or the officer's designee) blanket permission to "inspect and access [his] computer at any time,"[50] extinguish his expectation of privacy? *Third*, does the fact that DiTomasso never received the emails — because they were

---

[47] *See Schneckloth*, 412 U.S. at 241-42 (explaining the differences between criminal procedure rights associated with trial, and criminal procedure rights associated with search). *See also Ohio v. Robinette*, 519 U.S. 33 (1996) (holding, inter alia, that a search can be consented to even if a defendant to be advised that he is "free to go"); *United States v. Drayton*, 536 U.S. 194 (2002) (holding that a search can be consented to even if a defendant does not subjectively feel free to leave).

[48] *Garcia*, 56 F.3d at 422.

[49] *Florida v. Jimeno*, 500 U.S. 248, 250 (1991).

[50] Probation Order at 2 ¶ U.

quarantined by AOL — deprive him of standing to raise a Fourth Amendment challenge?

1. Expectations of Privacy in Electronic Communications Generally

The government offers multiple theories why DiTomasso had no expectation of privacy in his electronic communications. *First*, the government maintains that by "broadcast[ing] his statements in the presence of others"[51] — that is, by exchanging emails and chats with other people — DiTomasso relinquished his expectation of privacy in those statements. This argument is baseless. Although the government is correct that "when an individual reveals private information to another, he assumes the *risk* that his confidant will reveal [it] to the authorities,"[52] it does not follow that no expectation of privacy exists. In fact, just the opposite: it only make sense to speak of a betrayed expectation of privacy insofar as one *has* an expectation of privacy. The government's reliance on the "misplaced confidence" cases is not helpful.

On the government's logic, if DiTomasso were to disclose private information to a friend over the phone — which, by the nature of the act, would

---

[51] Opp. Mem. at 11.

[52] *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) (emphasis added).

cause DiTomasso to "assume[] the risk" that his friend might relay the information to law enforcement — he would have no expectation of privacy in the phone call, and no Fourth Amendment protection would apply. This reasoning was rejected by the Supreme Court in *Katz v. United States*,[53] when it held that disclosing information to someone else does *not* automatically permit intrusion (in particular, wiretapping) by law enforcement. To this day, *Katz* remains a "lodestar" of Fourth Amendment law.[54]

Second, the government argues that even if DiTomasso had an expectation of privacy in the emails, the same is not true of the chats, because the latter occurred in "a public chat room, which was open to all who cared to enter."[55] The government likens DiTomasso's "statements in [the Omegle chatroom]" to "those made loudly . . . while standing in a town square"[56] — a category of disclosure that clearly falls beyond the scope of Fourth Amendment protection.

This argument misunderstands how Omegle works. Although the company adopts the term "chatroom" to refer to its online platform, that platform is

---

[53] *See Katz*, 389 U.S. at 356-57.

[54] *Smith*, 422 U.S. at 740.

[55] Opp. Mem. at 11.

[56] *Id.*

"a far cry from the public chat rooms that were popular [] years ago," in which "a user [knew] that his comments are out there for the rest of the world to see."[57] Indeed, the whole point of Omegle's service is to allow two strangers to chat anonymously, and only with one another. For Fourth Amendment purposes, there is no distinction between an Omegle chat and an email correspondence — or for that matter, between an Omegle chat and a phone call. Both involve one-on-one interactions that users clearly expect to be kept private.

Third, the government suggests that DiTomasso had no expectation of privacy in his electronic communications because the ISPs responsible for facilitating those communications — AOL and Omegle — warned him that they might be "monitor[ing]" his activity.[58] Given DiTomasso's "clear and explicit" notice that AOL "reserved the right to . . . disclose[] the content of his communications to law enforcement, if [DiTomasso used] his email account for illegal activities,"[59] and that Omegle was using an "automated system" to "screen [DiTomasso's chats]" and potentially "share [them] with third parties, including

---

[57] DiTomasso's Reply Memorandum ("Rep. Mem."), at 5.

[58] Opp. Mem. at 13.

[59] *Id.* at 12.

law enforcement,"[60] the government argues that DiTomasso can claim no reasonable expectation that his emails and chats "would not be review[ed]."[61]

Along with the Sixth and Ninth Circuits, both of whom have addressed variations on this argument,[62] I conclude that it would subvert the purpose of the Fourth Amendment to understand its privacy guarantee as "waivable" in the sense urged by the government. In today's world, meaningful participation in social and professional life requires using electronic devices — and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social interaction or (2) the evisceration of the Fourth Amendment. Neither result is acceptable.

In her concurrence in *United States v. Jones*, Justice Sonia Sotomayor wrote that in "the digital age," people tend to "reveal a great deal of information

---

60 *Id.* at 13.

61 *Id.* at 12.

62 *See United States v. Warshak*, 490 F.3d 455 (6th Cir. 2007) (holding that users have a reasonable expectation of privacy in the content of stored email), *vacated en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008) (holding that users have reasonable expectation of privacy in text messages, despite advance warning that the messages could be read), *rev'd on other grounds*, 560 U.S. 746 (2010).

about themselves to third parties in the course of carrying out mundane tasks," making it "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[63] Justice Sotomayor is certainly correct. But even beyond that, the "premise" to which she refers — that "an individual has no expectation of privacy in information voluntarily disclosed to third parties" — is not nearly as strong, in Fourth Amendment jurisprudence, as the government implies.

For example, the Supreme Court has held that employees, including public employees, enjoy an expectation of privacy in their workplace desks — and that the expectation stays intact vis-a-vis law enforcement *even if* it would be unreasonable, given the "operational realities" of the workplace, for employees to expect the same privacy protection from their supervisors.[64] In other words, when employees constructively consent to searches by their supervisors, it does not automatically follow that they also consent to searches by law enforcement.

---

[63] *United States v. Jones*, 132 S.Ct. 935, 957 (2012) (Sotomayor J., concurring).

[64] *See O'Conner v. Ortega*, 480 U.S. 709, 117-18 (1987) ("[Although] [t]he operational realities of the workplace [] may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official . . . [the] [c]onstitutional protection against unreasonable searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer.").

Similarly, in the context of hotels, it is well-established that granting hotel management access to one's room for limited purposes — for example, in case of emergency, or for housekeeping — neither vitiates one's expectation of privacy in the room nor authorizes hotel employees to consent to a search by the government on behalf of the guest.[65]

Both of these holdings cut against the government's position. In essence, the government argues that by consenting to have his emails and chats searched by AOL and Omegle — as DiTomasso arguably did when he agreed to their respective terms of use — he *also* consented to permitting the government to search. Fourth Amendment privacy, however, is a context-sensitive question of societal norms. In some domains, people expect information to stay shielded from law enforcement even as they knowingly disclose it to other parties. As the Supreme Court has recognized, workplace desks and hotel rooms are two such domains. In the digital age, electronic communication is another.

Moreover, the lower-court cases that the government cites — *United States v. Hagood*, from the Northern District of California, and *United States v.*

---

[65] *See Stoner v. California*, 376 U.S. 483 (1964) (holding that searches of hotel rooms are subject to Fourth Amendment scrutiny despite the fact that "when a person [rents] a [] room he undoubtedly gives 'implied or express permission' to 'such persons as maids, janitors or repairmen' to enter his room 'in the performance of their duties,'") (internal citations omitted). *See also Chapman v. United States*, 365 U.S. 610 (holding the same with respect to an apartment).

Carabello, from the District of Vermont — do not support its position. Neither case holds that users lack an expectation of privacy in the contents of digital communication. Rather, both cases are about expectations of privacy in the *metadata* of digital communication. In *Hagood*, the court held that the defendant had no expectation of privacy in his IP address because an IP address is "analog[ous] [] to the outside of a letter, and the monitoring of an IP address [is analogous to] a pen register."[66] Similarly, in *Carabello*, the court held that the defendant had no expectation of privacy in the location information generated by his cell phone.[67] These cases do not support the proposition that DiTomasso lacked an expectation of privacy in the *content* of his emails and chats.[68]

---

[66] *United States v. Hagood*, No. 13 Cr. 393, 2014 WL 2918271, at *2 (N.D.Cal. June 26, 2014).

[67] *See United States v. Carabello*, 963 F. Supp. 2d 341, 361 (D.Vt. 2013). *But see In re United States for An Order Authorizing The Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (holding that Fourth Amendment protection extends to cell-site location records).

[68] With respect to one of the electronic communications in dispute — the email hashed by IDFP, forming the basis of NCMEC report #1558963 — it appears that only the metadata was examined. Unlike the "photoDNA" program, which hashes for image and video attachments that are "similar" to known child pornography — and requires an AOL employee to screen the file manually — IDFP only finds exact matches, making it possible to send "an automatic report to [NCMEC]" without human review. Phillips Decl. ¶¶ 7, 11. In essence, IDFP is a mechanism for flagging images and videos that have already been transmitted through AOL, which means that the file is already known to be illicit.

To challenge the constitutionality of AOL's IDFP hashing program,

2. DiTomasso's Probation Agreement Does Not Extinguish His Expectation of Privacy

The government argues that DiTomasso's expectation of privacy in his computer — and by extension, in his emails and chats — was "severely diminished" by his probation agreement,[69] which gave his "probation officer or their designee" blanket license to "inspect and access [DiTomasso's] computer at anytime, [] includ[ing] storage devices and other media."[70]

Even supposing the government is right, however, it requires a significant leap to conclude that DiTomasso had *no* expectation of privacy in his computer. Were that so, any government actor could continually surveil all of DiTomasso's electronic communications without ever triggering Fourth Amendment scrutiny. This would be a radical extension of existing case law. If

---

DiTomasso must claim an expectation of privacy not in the *content* of his email, but rather in the "hash number" of an attached file. Whether he can do so is unclear: the constitutional status of digital metadata is currently in flux. *Compare ACLU v. Clapper*, 959 F. Supp. 2d 724, 749-53 (S.D.N.Y. 2013) (holding, under *Smith*, that individuals do not have a reasonable expectation of privacy in telephony metadata), *with Klayman v. Obama*, 957 F. Supp. 2d 1, 32 (D.D.C. 2013) ("I am convinced that the surveillance program now before me is so different from a simple pen register [in] *Smith* . . . that bulk telephony metadata collection and analysis [violates] a reasonable expectation of privacy."). Because I conclude that DiTomasso consented to law enforcement search of his emails when he agreed to AOL's terms of use, no ruling on the metadata issue is necessary.

[69] Opp. Mem. at 13.

[70] Probation Order at 2 ¶ U.

anything, the probation search cases are about a probationer's expectations of privacy vis-a-vis his *probation* officer, not vis-a-vis all law enforcement.[71] And even then, it is unclear whether probationers have *no* expectation of privacy from their probation officers — or whether Fourth Amendment protection still applies, but in an attenuated fashion.[72]

If it had been DiTomasso's probation officer who examined his chat history, or who looked through his emails, this might well be a different case. As it stands, however, I cannot conclude that DiTomasso's probation agreement extinguished his expectations of privacy vis-a-vis law enforcement in general.

3. AOL's Interception of DiTomasso's Emails Does Not Vitiate His Expectation of Privacy

Finally, the government argues that DiTomasso does not have

---

[71] *See Reyes*, 283 F.3d at 462 (focusing exclusively on home visits and searches by probation officers, not by law enforcement in general).

[72] In the Second Circuit, the rule is that consent-to-search provisions attenuate, but do not destroy, the need for a baseline level of suspicion in searches by probation officers. *See Lifshitz*, 369 F.3d at 181-82 (explaining that consent-to-search terms in probation agreements lessen expectations of privacy, but they do not give probation officers carte blanche to perform truly suspicionless searches); *Newton*, 369 F.3d at 665 (holding that probationers who sign consent-to-search agreements have a "'severely diminished expectation of privacy'" in connection with their "supervision" by probation officers) (quoting *Reyes*, 283 F.3d at 461). *See also Knight*, 534 U.S. at 119-20 (explicitly reserving the question of whether a consent-to-search provision in a probation agreement "diminishe[s], or completely eliminate[s], [the probationer's] expectation of privacy").

"standing" to challenge the search of emails that "[he] never received."[73] In other words, "[b]ecause [DiTomasso] has not shown that he had any reasonable expectation of privacy in the emails of another that never came into his possession," he cannot raise a Fourth Amendment claim.[74]

This arguments fails. For Fourth Amendment purposes, there is no basis for treating *recipients* of email differently from *senders* of email. Both have a reasonable expectation of privacy in the content of correspondence. If the government's reasoning were correct, law enforcement officers could read a user's incoming email with impunity, so long as they made sure to divert it from the user's inbox before doing so. In other words, on the government's logic, a search that might otherwise be subject to Fourth Amendment scrutiny — were the email in the recipient's inbox — would escape Fourth Amendment scrutiny if law enforcement took the added step of seizing the email outright.

This, as DiTomasso rightly puts it, "is completely antithetical to the general public's expectations of privacy."[75] Although he cites no case law squarely on point — and I have not been able to locate any — the reason for the lack of

---

[73] Opp. Mem. at 12.

[74] *Id.*

[75] Rep. Mem. at 3.

authority is clear. The government's position is untenable.

Nevertheless, a helpful parallel arises in cases involving the surveillance of prisoner mail. There, courts have assumed that prisoners have a privacy interest in *all* mail, regardless of whether it is incoming or outgoing — and any Fourth Amendment analysis proceeds from that assumption. If prisoners have an expectation of privacy in their incoming mail, it follows *a fortiori* that free citizens do as well.[76] Furthermore, for the purposes of this inquiry — whether recipients, in addition to senders, enjoy an expectation of privacy in their correspondence — there is no difference between regular mail and email. The same holds for both. DiTomasso has standing, as the intended recipient of the emails hashed and quarantined by AOL, to raise a Fourth Amendment claim.

B. DiTomasso Consented to Search of His Emails, But Not His Chats

Having established that DiTomasso had an expectation of privacy in the content of his electronic communications, the final question the Court must resolve is whether DiTomasso consented to a search of those communications by law enforcement. Because consent cases typically involve encounters between citizens and police officers, the voluntariness of agreement is often a source of

---

[76] *See, e.g.*, *United States v. Felipe*, 148 F.3d 101, 107-08 (2d Cir. 1998) (assuming that the defendant, while in prison, had an expectation of privacy in both incoming and outgoing mail).

controversy. Here, by contrast, there is no question that DiTomasso voluntarily agreed to AOL's and Omegle's policies. The only question is *what* he consented to by doing so.

As the Supreme Court has explained, this question should be answered "objective[ly]" — by reference to what a "typical reasonable person [would understand]" AOL's and Omegle's policies to mean.[77] Furthermore, to hold that DiTomasso waived his Fourth Amendment rights with respect to the monitoring of his chats or emails, it is not enough to conclude that the policies contemplated a search by AOL or Omegle in their capacity as private entities. Rather, to hold that DiTomasso waived his Fourth Amendment rights, it would be necessary to conclude that the policies contemplated a search by AOL or Omegle in a *law enforcement* capacity. Put otherwise, because DiTomasso's constitutional claim rests on the proposition that AOL and Omegle were acting as government agents when they monitored his electronic communications, the policies only defeat his constitutional claim if, by agreeing to them, he was consenting to a search by AOL and Omegle *as* government agents.

Omegle's policy makes two references to "law enforcement."[78] *First*,

---

[77] *Jimeno*, 500 U.S. at 250.

[78] Omegle Policy at 1.

it puts users on notice that "Omegle keeps a record of the IP addresses involved in every chat," and that those "records are intended to be used for the purpose of law enforcement."[79] *Second*, at its conclusion, the policy reiterates that Omegle "may [] share[] with third parties for the purposes of law enforcement" the "records" that it keeps,[80] though the log of IP addresses is the only "record" mentioned. In other sections, the policy also explains that Omegle reserves the right — for "quality control purposes"[81] — to monitor user chats for the purposes of (1) filtering spam and (2) ferreting out "misbehavior."[82]

On these facts, I cannot conclude that DiTomasso consented to a search by Omegle in a law enforcement capacity. Omegle took snapshots of DiTomasso's chats and parsed them for content. Although that form of monitoring *is* referenced in the policy, it is mentioned exclusively as a means of "monitoring for misbehavior"[83] — by which the policy clearly means violations of Omegle's rules, not criminal activity — and of improving Omegle's internal monitoring

---

79 *Id.*

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

system.[84]

A reasonable person, having read carefully through the policy, would certainly understand that by using Omegle's chat service, he was running the risk that another party — including Omegle — might divulge his sensitive information to law enforcement. But this does not mean that a reasonable person would also think that he was consenting to let Omegle freely monitor his chats if Omegle was working *as an agent* of law enforcement. When Omegle's policy refers to the "law enforcement [purpose]" behind maintaining IP address records, it is unclear whether this "purpose" is motivated (1) by Omegle's independent desire to aid criminal investigations, or (2) by Omegle's obligations under state or federal law. In other words, it is plausible to interpret the policy as implying that Omegle is *required* to keep IP address records. So construing the policy, a reasonable user would be unlikely to conclude that Omegle intended to act as an agent of law enforcement. And such a user would be even *less* likely to conclude that he had agreed to permit such conduct.

---

[84] *See id.* (explaining that snapshots of chats are sometimes "stored and used to improve Omegle's monitoring process"). Not only does the policy itself distinguish between IP address records (kept for law enforcement purposes) and the monitoring of chats (for quality control purposes) — this distinction also tracks Fourth Amendment doctrine. Unlike the content of chats, IP addresses are metadata, in which DiTomasso would have a far more limited expectation of privacy, if any.

AOL's policy is quite different. Not only does it explicitly warn users that criminal activity is disallowed,[85] and that AOL monitors for such activity; the policy also explains that "AOL reserves the right to take any action it deems warranted" in response to illegal behavior, including "terminat[ing] accounts and cooperat[ing] with law enforcement."[86] The policy also makes clear that AOL reserves the right to reveal to law enforcement information about "crimes[s] that [have] been or [are] being committed."[87] In contrast to Omegle's policy, which includes only a passing reference to law enforcement — and which gives no indication of the role Omegle intends to play in criminal investigations — AOL's policy makes clear that AOL intends to actively assist law enforcement. For this reason, I conclude that a reasonable person familiar with AOL's policy would understand that by agreeing to the policy, he was consenting not just to monitoring by AOL as an ISP, but also to monitoring by AOL as a government agent. Therefore, DiTomasso's Fourth Amendment challenge fails as to the emails.

IV. CONCLUSION

For the foregoing reasons, I conclude that DiTomasso had a

---

85 *See* AOL Terms of Service at 1.

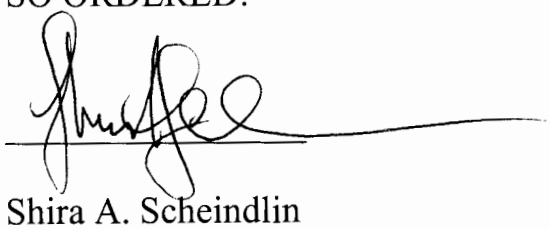
86 AOL Guidelines at 1-2.

87 AOL Privacy Policy at 2.

reasonable expectation of privacy in the contents of his Omegle chats as well as his AOL emails. However, by agreeing to AOL's terms of service, DiTomasso consented to a search of his AOL emails by law enforcement, thereby waiving his Fourth Amendment rights. Therefore, the two NCMEC reports arising from DiTomasso's AOL emails, #1560137 and #1558963 — as well as any other evidence gathered as a result of those reports — are admissible under the Fourth Amendment.

The constitutional status of NCMEC reports #1704143, #1741964, and #2235394 — the reports resulting from Omegle chats — remains unresolved. The next question this Court must address is whether Omegle's monitoring of DiTomasso's chats was a "private search," outside the bounds of constitutional protection, or whether it was a search carried out at the behest of law enforcement, which would trigger Fourth Amendment scrutiny. Because DiTomasso addressed this issue in his initial memorandum, and the government has offered a response in opposition, DiTomasso is ordered to submit a supplemental reply, of no more than ten pages and limited to the private search issue, by November 3, and the government is ordered to submit a supplemental sur-reply, also of no more than ten pages and limited to the private search issue, by November 10. A suppression hearing is scheduled for November 13 at 10 AM.

SO ORDERED:



Shira A. Scheindlin
U.S.D.J.

Dated: New York, New York
October 28, 2014

- Appearances -

For Defendant Frank DiTomasso:

Lee Ginsberg, Esq.
Nadjia Limani, Esq.
Freeman, Nooter & Ginsberg
75 Maiden Lane, Suite 503
New York, NY 10038
(212) 608-0808

For the Government:

Margaret Graham
Assistant U.S. Attorney
U.S. Attorney's Office for the Southern District of New York
One Saint Andrew's Plaza
New York, NY 10007
(212) 637-2923